UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,898	01/31/2002	Manish Patel	DIGITAL 3.0-001	5961

27614 7590 08/05/2005

MCCARTER & ENGLISH, LLP
FOUR GATEWAY CENTER
100 MULBERRY STREET
NEWARK, NJ 07102

EXAMINER	
PEARSON, DAVID J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/062,898	PATEL ET AL.	
	Examiner	Art Unit	
	David J. Pearson	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/31/2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/28/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

1. Claims 1-28 have been examined.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

2. The abstract of the disclosure is objected to because it exceeds 150 words in length. Correction is required. See MPEP § 608.01(b).

Claim Objections

3. Claims 3-19 objected to because of the following informalities: Claim 3 recites, "... the confidential data remaining mixed after said step (D) of isolating the first biometric data, said step (C) of decrypting including..." The claim is difficult to read without an "and" or a semicolon separating the items in the list. Claims 4-19 introduce no new problems, but inherit the objection of claim 3. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-10, 13-14, 18-20 and 24-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Rahman et al (U.S. Patent Application Publication 2002/0144128).

For claim 1, Rahman et al. teach a method for communicating confidential data from a sender to a receiver, comprising the steps of:

(A) encrypting the confidential data while the confidential data is in the control of the sender, said step of encrypting including mixing the confidential data with biometric data to produce encrypted data (note paragraph [0037]);

(B) sending the encrypted data over a communication link to the receiver (note paragraph [0028]);

(C) de-encrypting the encrypted data while the encrypted data is in the control of the receiver by separating the biometric data from the confidential data (note paragraph [0037]).

For claim 2, Rahman et al. teach a method of claim 1, wherein the biometric data includes first biometric data relating to the receiver (note paragraphs [0132] and [0186]) and further including the steps of:

(D) isolating the first biometric data from the encrypted data after said step of sending (note paragraph [0038]);

(E) generating second biometric data relating to the receiver (note paragraph [0038]); and

(F) comparing the first biometric data to the second biometric data to determine if there is a predetermined level of similarity there between, said steps of isolating, generating and comparing being conducted prior to said step of de-encrypting, with the execution or non-execution of said step of de-encrypting being dependent upon whether the predetermined level of similarity is present (note paragraphs [0025] and [0038]).

For claim 3, Rahman et al. teach a method of claim 2, wherein said step (A) of encrypting includes mixing an additional data component with the confidential data and the first biometric data to produce the encrypted data, the additional data component and the confidential data remaining mixed after said step (D) of isolating the first biometric data; said step (C) of de-encrypting including separating the confidential data from the additional data component (note paragraph [0037]).

For claim 4, Rahman et al. teach a method of claim 3, wherein the additional data component includes secret key data (note paragraph [0037]).

For claim 5, Rahman et al. teach a method of claim 4 wherein the secret key data is combined with the confidential data via a logical/mathematical operation to encrypt said confidential data (note paragraph [0035]).

For claim 6, Rahman et al. teach a method of claim 5, wherein the secret key data is combined with the confidential data before said step of mixing the confidential data with the biometric data in said step (A) (note paragraph [0037]).

For claim 7, Rahman et al. teach a method of claim 6, wherein the secret key data is de-combined from the confidential data after said step of separating the biometric data from the confidential data is said step (C) (note paragraph [0037]).

For claim 8, Rahman et al. teach a method of claim 7, wherein the secret key data is combined with the biometric data via a logical/mathematical operation to encrypt the biometric data (note paragraph [0027]) and wherein the secret key data is de-combined from the biometric data after said step of separating the biometric data from the confidential data in said step (C) (note paragraph [0037]).

For claim 9, Rahman et al. teach a method of claim 8, further including the step of deriving the secret key data from a password via a predefined logical/mathematical formula (note paragraph [0032]).

For claim 10, Rahman et al. teach a method of claim 5, wherein the secret key data is combined with the biometric data via a logical/mathematical operation to encrypt said biometric data (note paragraph [0027]).

For claim 13, Rahman et al. teach a method of claim 3, wherein the first biometric data is a reference voice signature of the receiver and further comprising the steps of:

(I) producing the reference voice signature for the receiver (note paragraph [0024]);

(J) storing the reference voice signature produced in step (I) (note paragraph [0024]); and

(K) communicating the reference voice signature of the receiver to the sender prior to said step (A) of encrypting the confidential data (note paragraph [0026]).

For claim 14, Rahman et al. teach a method of 13, wherein the reference voice signature is stored on a server computer on the Internet (note paragraph [0023]) and said step (K) of communicating includes downloading the reference voice signature from the server computer to a sender computer available to the sender (note paragraph [0023]).

For claim 18, Rahman et al. teach a method of claim 13, wherein said step (E) of generating includes deriving a voice signature from a speech sample given in real time by the receiver (note paragraph [0132]).

For claim 19, Rahman et al. teach a method of claim 18, wherein said step (E) of generating includes the receiver speaking into an audio input of a computer to provide a speech sample, the speech sample being processed by the computer to derive the voice signature (note paragraphs [0023] and [0024]).

For claim 20, Rahman et al. teach a method of claim 1, wherein the confidential data is in the form of a computer file residing on a first computer controlled by the sender (note paragraph [0033]), wherein the communication link is a computer network and said step of sending includes sending the encrypted data over the computer network to a second computer in the control of the receiver (note paragraph [0028]).

For claim 24, Rahman et al. teach a method of claim 24, wherein the computer network includes the Internet and said step (B) of sending includes the transfer of the encrypted data from the first computer to a server computer and from the server computer to the second computer (note paragraph [0028]).

For claim 25, Rahman et al. teach a method for encrypting and de-encrypting confidential data, comprising the steps of:

(A) encrypting the confidential data by combining the confidential data with secret key data in accordance with a first predetermined logical/mathematical algorithm to produce data at a first level of encryption (note paragraph [0037]);

(B) obtaining biometric data relating to a living creature (note paragraph [0024]);

(C) mixing the biometric data with the data at the first level of encryption in accordance with a second predetermined algorithm to produce data at a second level of encryption (note paragraph [0037]);

(D) de-encrypting the data at the second level of encryption by separating the data at the second level of encryption with the biometric data and the data at the first level of encryption using the second pre-determined algorithm in reverse (note paragraph [0037]); and

(E) de-combining the confidential data and the secret key data using the reverse of the first predetermined logical/mathematical algorithm (note paragraph [0037]).

5. Claims 1-3, 11-14 and 18-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Talmor et al (U.S. Patent Application Publication 2003/0135740).

Talmor et al. teach a method for communicating confidential data from a sender to a receiver, comprising the steps of:

(A) encrypting the confidential data while the confidential data is in the control of the sender, said step of encrypting including mixing the confidential data with biometric data to produce encrypted data (note paragraph [0203]);

(B) sending the encrypted data over a communication link to the receiver (note paragraph [0107]);

(C) de-encrypting the encrypted data while the encrypted data is in the control of the receiver by separating the biometric data from the confidential data (note paragraph [0213]).

For claim 2, Talmor et al. teach a method of claim 1, wherein the biometric data includes first biometric data relating to the receiver (note paragraphs [0132] and [0186]) and further including the steps of:

(D) isolating the first biometric data from the encrypted data after said step of sending (note paragraph [0205]);

(E) generating second biometric data relating to the receiver (note paragraph [0209]); and

(F) comparing the first biometric data to the second biometric data to determine if there is a predetermined level of similarity there between, said steps of isolating, generating and comparing being conducted prior to said step of de-encrypting (note paragraph [0210]), with the execution or non-execution of said step of de-encrypting being dependent upon whether the predetermined level of similarity is present (note paragraph [0211]).

For claim 3, Talmor et al. teach a method of claim 2, wherein said step (A) of encrypting includes mixing an additional data component with the confidential data and the first biometric data to produce the encrypted data, the additional data component and the confidential data remaining mixed after said step (D) of isolating the first biometric data; said step (C) of de-encrypting including separating the confidential data from the additional data component (note paragraph [0203]).

For claim 11, Talmor et al. teach a method of claim 3, wherein the additional data component is third biometric data (note paragraph [0203]).

For claim 12, Talmor et al. teach a method of claim 11, wherein the third biometric data is a voice signature of the sender and further including the steps of:

(G) producing a reference voice signature for the sender (note paragraph [0132]); and

(H) storing the reference voice signature produced in step (G), prior to said step (A) of encrypting the confidential data (note paragraph [0130]).

For claim 13, Talmor et al. teach a method of claim 3, wherein the first biometric data is a reference voice signature of the receiver and further comprising the steps of:

(I) producing the reference voice signature for the receiver (note paragraph [0132]);

(J) storing the reference voice signature produced in step (I) (note paragraph [0130]); and

(K) communicating the reference voice signature of the receiver to the sender prior to said step (A) of encrypting the confidential data (note paragraph [0186]).

For claim 14, Talmor et al. teach a method of 13, wherein the reference voice signature is stored on a server computer on the Internet (note paragraph [0096]) and said step (K) of communicating includes downloading the reference voice signature from the server computer to a sender computer available to the sender (note paragraph [0186]).

For claim 18, Talmor et al. teach a method of claim 13, wherein said step (E) of generating includes deriving a voice signature from a speech sample given in real time by the receiver (note paragraph [0132]).

For claim 19, Talmor et al. teach a method of claim 18, wherein said step (E) of generating includes the receiver speaking into an audio input of a computer to provide a speech sample, the speech sample being processed by the computer to derive the voice signature (note paragraph [0132]).

For claim 20, Talmor et al. teach a method of claim 1, wherein the confidential data is in the form of a computer file residing on a first computer controlled by the

sender (note paragraph [0192]), wherein the communication link is a computer network and said step of sending includes sending the encrypted data over the computer network to a second computer in the control of the receiver (note paragraph [0200]).

For claim 21, Talmor et al. teach a method of claim 20, further including the step of:

(L) converting the encrypted data from a first file format to a second file format before said step (B) of sending (note paragraph [0200]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Talmor et al. as applied to claim 14 above, and further in view of Johnston.

For claim 15, Talmor et al. differ from the claimed invention in that they fail to specify the voice signature stored on the server has a flag that indicates the necessity of the receiver to authorize the sender before receiving confidential data from the sender, further including the step of checking the status of the flag prior to downloading the voice signature.

Johnston teaches a biometric certificate server where "Certificate access will initially be via X.400 and SMTP e-mail, with WWW access coming soon. USPS does not plan to allow unrestricted public access to the certificate database. In USPS operated X.500 servers the certificates would be in a private directory. Their model is that they will have "listed" and "unlisted" certificates. Listed certificates may be obtained by anyone, but only when requested by name (i.e. you have to know the distinguished name, you cannot "browse" the certificate database). Unlisted certificates can only be obtained from the certified entity (i.e. only the "owner" will distribute unlisted certificates, but they will be signed by the CA)."

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have formed the device of Talmor et al. using "listed" and "unlisted" certificates because it would improve the privacy of the users of the system who chose to use unlisted certificates. Note it would be obvious to one of ordinary skill that the use of some sort of flag would be necessary to differentiate "listed" and "unlisted" certificates and that flag would need to be checked before a sender downloads the certificate. Also, since the method of Johnston requires the "owner" or receiver to distribute their unlisted certificate. By distributing their certificate, the receiver is authorizing the sender before receiving confidential data from the sender.

For claim 16, Talmor et al. teach a method of claim 15 wherein said step (B) of sending includes uploading the encrypted data from the sender computer to the server computer; storing the encrypted data on an email system on the server computer; and

downloading the encrypted data from the server computer to a receiver computer available to the receiver. Note paragraph [0193], which teaches the sender, can designate the encrypted file to be an attachment in the email programs Outlook or Outlook Express and paragraph [0199], which teaches the recipient can be picked from an email address book. This means the encrypted data travels from the sender, to an email server and then on to the receiver.

7. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Talmor et al. and Johnston as applied to claim 16 above, and further in view of Tipirneni (U.S. Patent 6,381,029).

Talmor et al. differ from the claimed invention in that they fail to specify the encrypted data is stored on the receiver computer for a predetermined time and then deleted automatically.

Tipirneni teach a confidential data transfer system where the transferred data is "automatically erased after twenty-four hours." Tipirneni notes, "One of ordinary skill in the art will appreciate that the automatic deletion feature can be configured for different time periods."

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have formed the device of Talmor et al. where the encrypted data was deleted from the receiver computer after a predetermined length of time because Tipirneni teaches this method "For confidentiality and security purposes."

8. Claims 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Talmor et al. as applied to claim 21 above, and further in view of ScramDisk.

For claims 22 and 23, Talmor et al. differ from the claimed invention in that they fail to specify the fail to specify that the encrypted data is converted into a wave file before sending and then the process of de-encrypting includes converting the wave file back to its previous format. Instead, Talmor et al. teach the encrypted data is converted into an XML document for sending and converted back by the receiver.

ScramDisk teaches an encryption method where information is "stored in the low bits of a WAV audio file."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the device of Talmor et al. which converts the encrypted data into a wave file before sending it, then converting the wave file back as part of the decryption process because of the added security of hiding encrypted data in plain sight. ScramDisk teaches "this WAV file can be sent by e-mail or carried on a diskette without attracting too much attention (since by casual hearing the WAV file sounds like the original sound file).

9. Claims 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rahman et al. as applied to claim 25 above, and further in view of ScramDisk.

For claims 26 and 27, Rahman et al. differ from the claimed invention in that they fail to specify the encrypted data is converted to a wave file before sending and then the process of de-encrypting includes converting the wave file back to its previous format.

ScramDisk teaches an encryption method where information is "stored in the low bits of a WAV audio file."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the device of Rahman et al. which converts the encrypted data into a wave file before sending it, then converting the wave file back as part of the decryption process because of the added security of hiding encrypted data in plain sight. ScramDisk teaches "this WAV file can be sent by e-mail or carried on a diskette without attracting too much attention (since by casual hearing the WAV file sounds like the original sound file).

For claim 28, Rahman et al. teach the method of claim 27, wherein said step (B) of obtaining includes generating a speech sample and deriving a voice signature from the speech sample constituting the biometric data (note paragraph [0024]), and further including verifying the voice signature after said step of separating by generating a second speech sample and deriving a second voice signature and comparing the voice signature of the biometric data to the second voice signature to determine a predetermined degree of similarity prior to said step of de-combining (note paragraph [0025]).

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David J. Pearson whose telephone number is (571) 272-0711. The examiner can normally be reached on Monday - Friday, 8:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER